Claims

What is claimed is:

1. In a server, a method comprising:

registering a first party as a party relying upon a second party's certificate;

revoking the second party's certificate after registering the first party; and

initiating communication with the first party to indicate that the second party's certificate has been revoked.

2. The method of claim 1 wherein revoking the second party's certification further comprises:

receiving a request to revoke the second party's certificate; and

revoking the second party's certificate in accordance with a revocation policy associated with the second party's certificate in response to the request.

3. The method of claim 2 wherein initiating communication with the first party further comprises sending a revocation message to a machine that is associated with the first party.

4. The method of claim 3 further comprising the machine associated with the first party verifying the authenticity of the revocation message and modifying access control information of the machine to indicate the revocation of the second party's certificate.

5. The method of claim 2 wherein accepting the request to revoke the second party's certificate comprises accepting the request by authenticating a signature incorporated in the request with one of a list of revoker certificates associated with the second party's certificate.

6. The method of claim 2 wherein the server initiating communication with a first party further comprises the server sending an email message to an email address for the first party.

7. In a server, a method comprising:

registering an user as a party relying upon a digital certificate for a web site, the certificate to verify messages from the web site;

receiving a request to revoke the digital certificate of the web site after registering the user;

authenticating the request in accordance with a pre-defined policy;

revoking the digital certificate of the web site in response to the request; and

initiating communication with the user to indicate that the digital certificate of the web site has been revoked.

8. The method of claim 7 wherein initiating communication with the user to indicate that the digital certificate of the web site has been revoked further comprises:

sending a message directly to a machine associated with the user, to indicate that the web site's digital certificate has been revoked.

9. The method of claim 8 further comprising, in the machine used by the user:

authenticating the message to verify that it was sent by the server; and

changing settings for web access to reflect the revocation of the digital certificate of the web site.

10. The method of claim 7 wherein authenticating the request in accordance with a pre-defined policy comprises authenticating a digital signature incorporated in the request

with a list of digital certificates previously defined as revoker certificates for the web site.

11. A processor based server system comprising:

a registration database to register a first party as a relying party for a second party's certificate;

a revocation module to revoke the second party's certificate after the first party is registered; and

an interface with a communication network to initiate communication to indicate to the first party that the second party's certificate has been revoked.

12. The processor based server of claim 11 further comprising:

a machine readable medium accessible from a processor of the server having stored thereon an acceptance policy in accordance with which a revocation request received via the interface may be accepted, and further having stored thereon a revocation policy in accordance with which the second party's certificate may be revoked.

13. The processor based server of claim 12, wherein the revocation module is operable to send a revocation message to a machine that is associated with the first party, via the interface.

14. A processor based server comprising:

a registration database to register a user as a relying party for a digital certificate of a web site, the certificate to verify messages from the web site;

a machine readable medium accessible from a processor of the server having stored thereon an acceptance policy in accordance with which a revocation request received via an interface to communication network may be accepted, and further having stored thereon a revocation policy in accordance with which the digital certificate of the web site may be revoked in response to the revocation request;

a revocation module to revoke the digital certificate of the web site in accordance with the revocation policy; and

an interface with a communication network to indicate to the user that the web site's certificate has been revoked.

15. The processor based server of claim 12, wherein the revocation module is operable to send a revocation message to a machine operable by the user to access the web site.

16. A machine readable medium having stored thereon data which when accessed by a machine cause the machine to perform the method of claim 1.

17. The machine readable medium of claim 16 having stored thereon further data which when accessed by the machine cause the machine to perform the method of claim 2.

18. The machine readable medium of claim 17 having stored thereon further data which when accessed by the machine cause the machine to perform the method of claim 3.

19. The machine readable medium of claim 18 having stored thereon further data which when accessed by the machine cause the machine to perform the method of claim 4.

20. The machine readable medium of claim 17 having stored thereon further data which when accessed by the machine cause the machine to perform the method of claim 5.

21. The machine readable medium of claim 17 having stored thereon further data which when accessed by the machine cause the machine to perform the method of claim 6.

22. A machine readable medium having stored thereon data which when accessed by a machine cause the machine to perform the method of claim 7.

23. The machine readable medium of claim 22 having stored thereon further data which when accessed by the machine cause the machine to perform the method of claim 8.

24. The machine readable medium of claim 23 having stored thereon further data which when accessed by the machine cause the machine to perform the method of claim 9.

25. The machine readable medium of claim 22 having stored thereon further data which when accessed by the machine cause the machine to perform the method of claim 10.